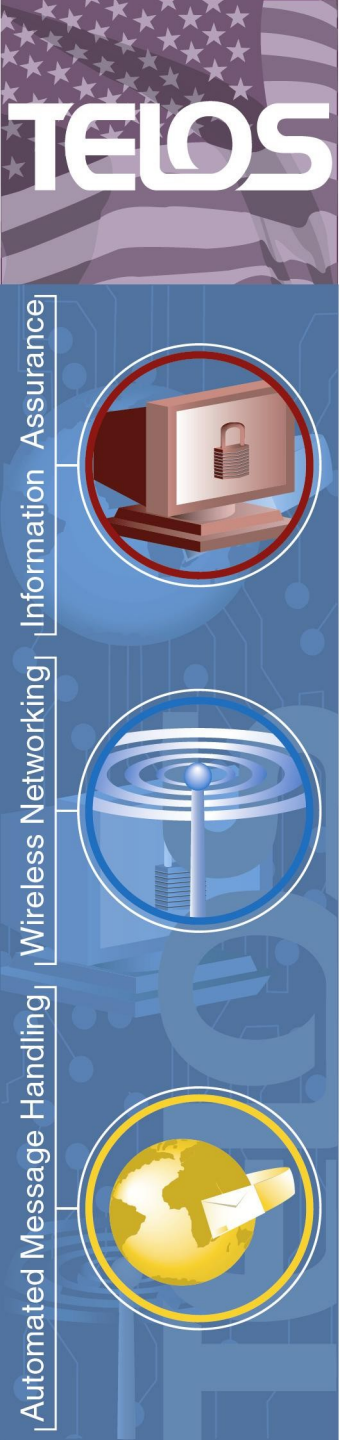
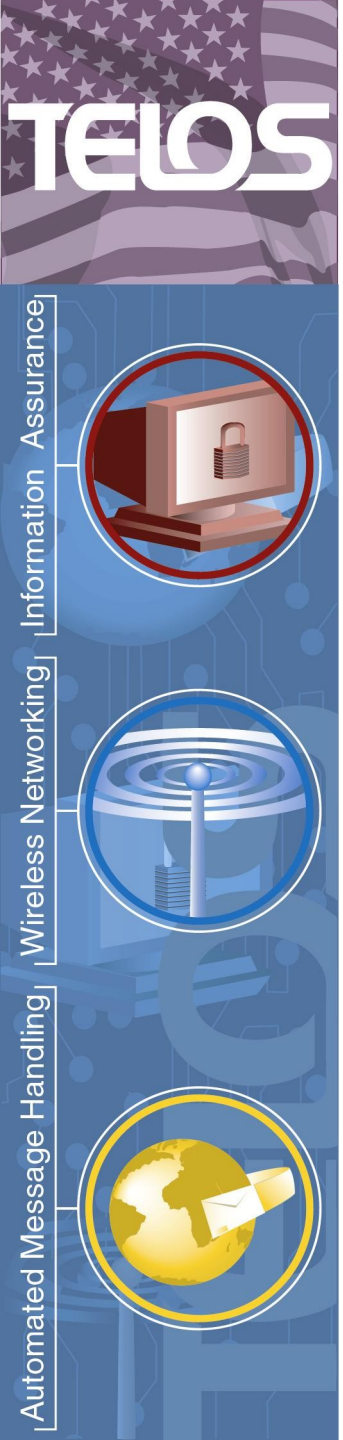


TELOS

Xacta Web C&A: Automating the Transition of DoN Legacy Systems/Applications to NMCI

Presented to the NMCI Industry Symposium

18 June, 2003



Agenda

- Legacy Applications/Systems/Networks and NMCI
- The Legacy System Transition Process
- Xacta Web C&A 4.0: Automate and Manage the Process

Achieving the full potential of NMCI

- The NMCI vision can only be fully realized when that network can support all the functions it takes to run the Navy
- This means integrating all the Navy specific applications and systems so they can run on NMCI
- Each NMCI site encounters many legacy systems/networks

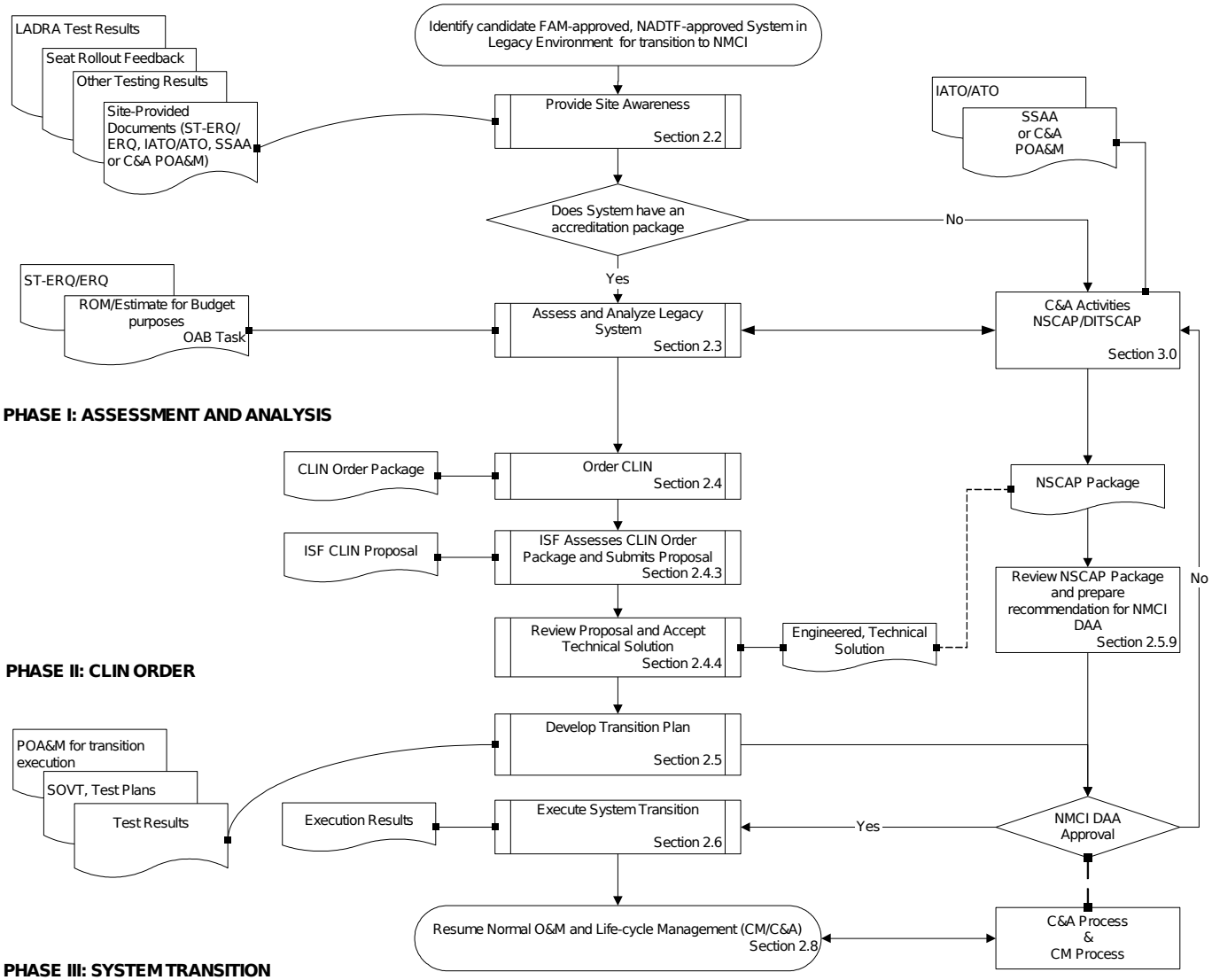
Who is Responsible for Legacy Applications?

- CIOs
- Central Design Activities
- Echelon 2 Commands
- Functional Area Managers

Transitioning to NMCI

- No “Free Lunch”
  - Transition the legacy application to run on the NMCI network (CLIN 29)
  - Gain NMCI connection approval for the legacy system/application (CLIN 27)
- All solutions require NSCAP (NMCI Security Certification and Accreditation Process) and/or DITSCAP
- Telos and Xacta can help

Transitioning the Legacy System



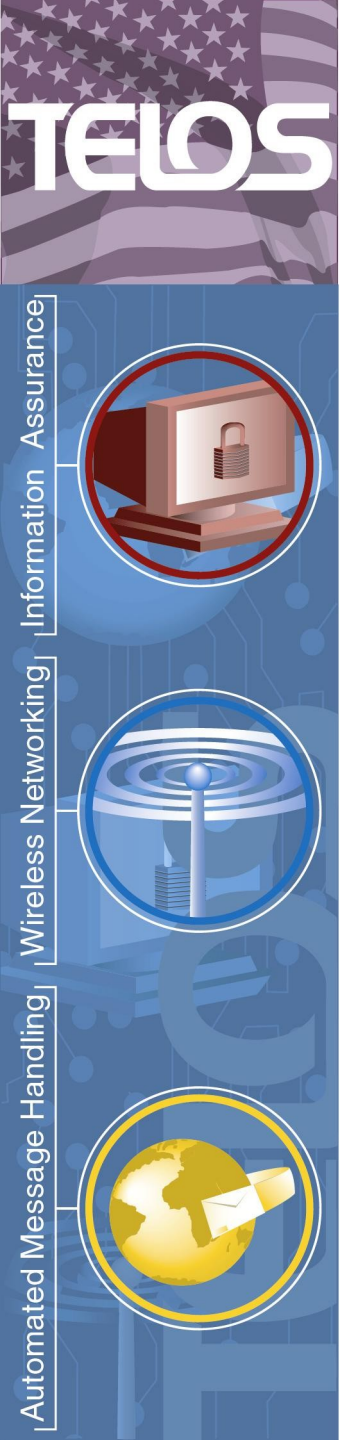
Information Assurance

Wireless Networking

Automated Message Handling

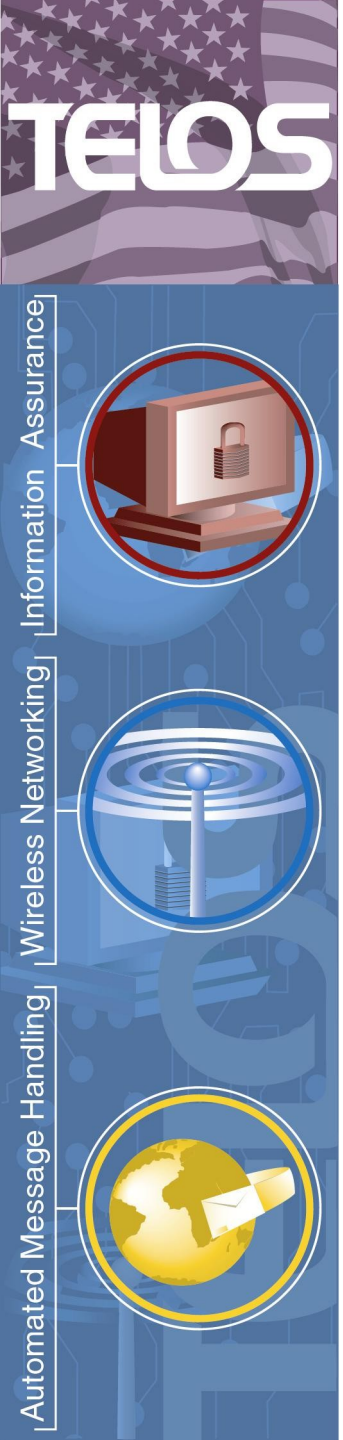
NMCI Specific Considerations

- Consider how the NMCI user will utilize your application
  - Browser only (Web-enabled per TFW)
  - NMCI Hosted
  - NMCI Connected
    - Your servers, your network connected to NMCI
  - Desktop element vs. Server / System
    - Site C&A for a single local instance
    - Type accreditation for enterprise deployment
  - Inside DMZ



NMCI Considerations cont.

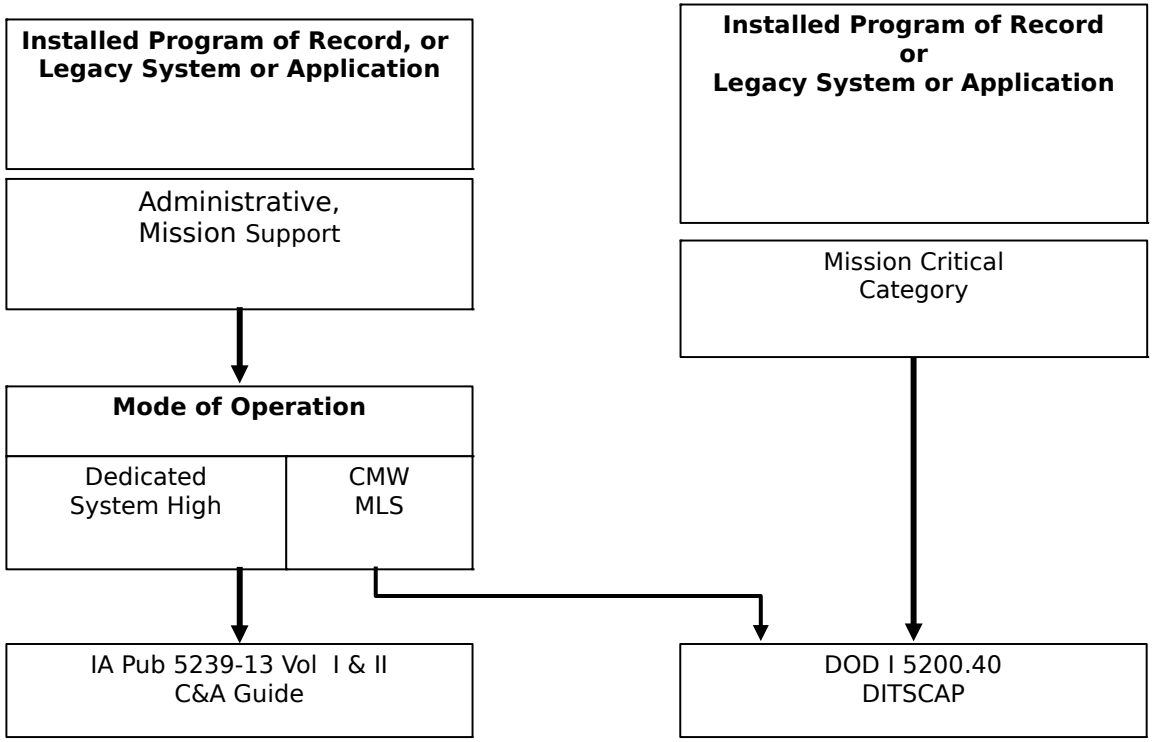
- NMCI enforces existing DON/DoD security policies
  - Navy IA Pub 5239-13 Vols. I-III
- NMCI requires a functional certification
- Resources (available at www.nmci.navy.mil)
  - NSCAP: NMCI Security Certification & Accreditation Process
  - LSTG: Legacy System Transition Guide (available soon)
  - NEADG: Navy Enterprise Application Developers Guide
  - NRDDG: NMCI Release Development and Deployment Guide



NSCAP

- Level of Effort is tailored based on
  - Mission criticality
  - Complexity
  - Mode of Operation
- May offer a more immediate path to IATO
  - Bridge to full DITSCAP and ATO, not a replacement
  - Some applications may go sunset before a full DITSCAP is needed
- Interpret and map accreditation requirements to systems/applications being transitioned

NSCAP C&A Level of Effort Guidance



NSCAP IA Requirements

Legacy System/Application Complexity	**Level of Effort For: Mission Support/ Administrative Systems**	**Level of Effort For: Mission Critical Systems**
Desktop/Client: Simple*	Requires: Risk Assessment •Functional and Security Certification Testing •Mobile Code Assessment	Requires: •Functional and Security Certification Testing •Mobile Code Assessment
Desktop/Client: Complex	Requires: Risk Assessment ** per Navy IA Pub 5239-13 Vol II (rev 01) •Checklist & Automated Vulnerability Assessment Tool •Functional and Security Certification Testing •B2 Firewall Baseline Configuration Compliance •Mobile Code Assessment •Navy Marine Corp NIPRNet Enclave Protection Policy Compliance	Requires: •Functional and Security Certification Testing •B2 Firewall Baseline Configuration Compliance •Mobile Code Assessment •Navy Marine Corp NIPRNet Enclave Protection Policy Compliance •DITSCAP ST&E and Risk Assessment •SSAA
Server Based/DBMS: Complex	Requires: Risk Assessment** per Navy IA Pub 5239-13 Vol II (rev 01) •Checklist & Automated Vulnerability Assessment Tool •Functional and Security Certification Testing •B2 Firewall Baseline Configuration Compliance •Mobile Code Assessment •Navy Marine Corp NIPRNet Enclave Protection Policy Compliance	Requires: •Functional and Security Certification Testing •B2 Firewall Baseline Configuration Compliance •Mobile Code Assessment •Navy Marine Corp NIPRNet Enclave Protection Policy Compliance •DITSCAP ST&E and Risk Assessment •SSAA

Telos/Xacta contribution

Legacy System/Application Complexity	Level of Effort For: Mission Support/ Administrative Systems	Level of Effort For: Mission Critical Systems
Desktop/Client: Simple*	Requires: Risk Assessment •Functional and ***Security Certification Testing*** •***Mobile Code Assessment***	Requires: •Functional and ***Security Certification Testing*** •***Mobile Code Assessment***
Desktop/Client: Complex	Requires: ***Risk Assessment** per Navy IA Pub 5239-13 Vol II (rev 01)*** •***Checklist & Automated Vulnerability Assessment Tool*** •Functional and ***Security Certification Testing*** •***B2 Firewall Baseline Configuration Compliance*** •***Mobile Code Assessment*** •***Navy Marine Corp NIPRNet Enclave Protection Policy Compliance***	Requires: •Functional and ***Security Certification Testing*** •***B2 Firewall Baseline Configuration Compliance*** •***Mobile Code Assessment*** •***Navy Marine Corp NIPRNet Enclave Protection Policy Compliance*** •***DITSCAP ST&E and Risk Assessment*** •***SSAA***
Server Based/DBMS: Complex	Requires: ***Risk Assessment** per Navy IA Pub 5239-13 Vol II (rev 01)*** •***Checklist & Automated Vulnerability Assessment Tool*** •Functional and ***Security Certification Testing*** •***B2 Firewall Baseline Configuration Compliance*** •***Mobile Code Assessment*** •***Navy Marine Corp NIPRNet Enclave Protection Policy Compliance***	Requires: •Functional and ***Security Certification Testing*** •***B2 Firewall Baseline Configuration Compliance*** •***Mobile Code Assessment*** •***Navy Marine Corp NIPRNet Enclave Protection Policy Compliance*** •***DITSCAP ST&E and Risk Assessment*** •***SSAA***

Xacta Web C&A

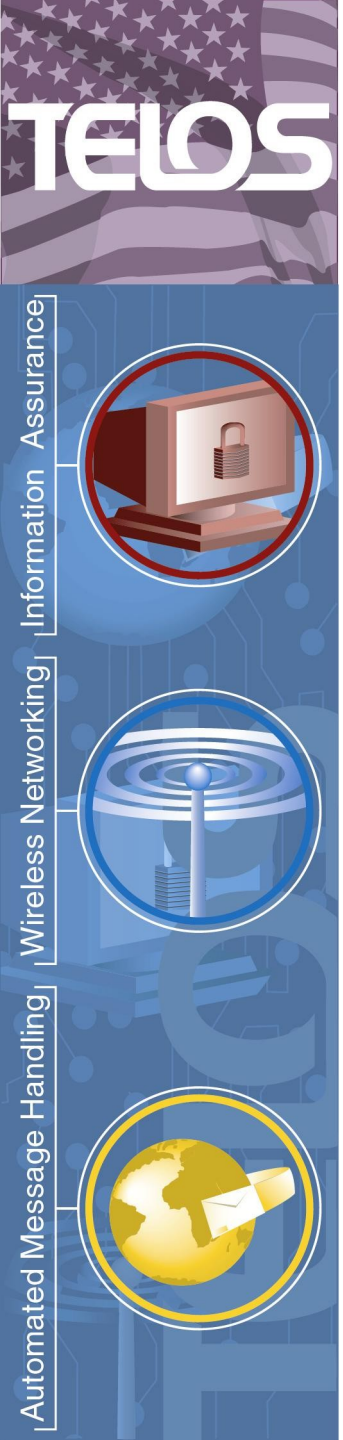
XWCA configured for NSCAP (Navy content and workflow, integration w/ other Navy tools like Securify)

Xacta on site support and services available through Telos (C&A, IA Services, Secure Software code audit, other IA products and services)

Information Assurance

Wireless Networking

Automated Message Handling

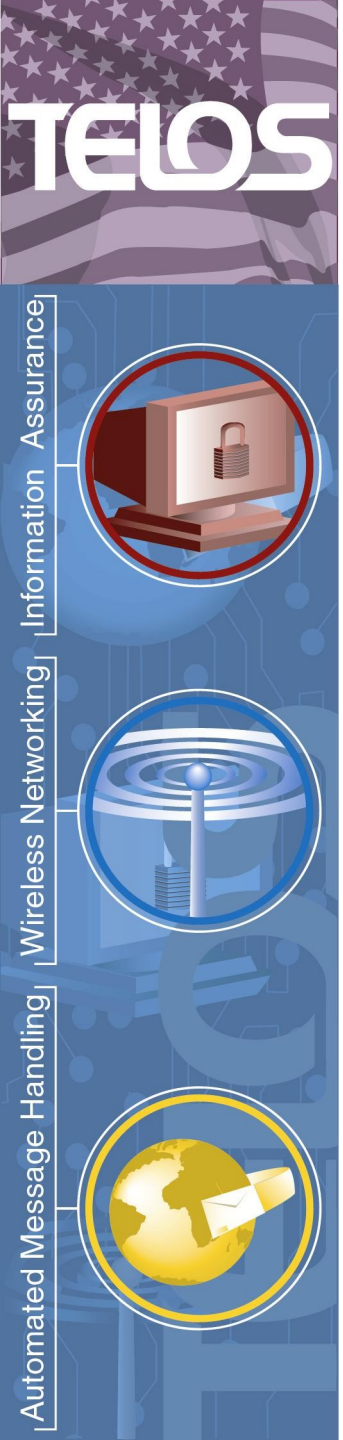


Telos/Xacta contribution

- Telos: 30+ years government experience
- Xacta (Telos subsidiary): 13+ years IA experience
- Xacta Web C&A
  - Mature product (version 4.0)
  - Evaluated and/or recommended and being piloted by DON Organizations
    - SPAWAR (PMO, IATT, PMW-161)
    - COMNAVNETWARCOM
      - "An enterprise tool to support C&A at the CDA and ISSM level is crucial for getting to and maintaining secure networks.“
      - Capt Bob Whitkop, COMNAVNETWARCOM N6, 1 April 2003
    - Director NMCI (PEO-IT)
      - APPLICATION SERVER MIGRATION PILOT Project
      - “The contractor shall validate the viability of Telos' Xacta Web technology as a Certification and Accreditation tool to be available to the enterprise as a centrally provided tool to track C&A data for all systems.”
  - Agency-wide adoption by: IRS, Army COE, Air National Guard, Dept. of Education

Xacta Web C&A Background

- Browser based software application designed to automate the security certification & accreditation (C&A) process
- The software includes
  - Auto-Discovery (Xacta Detect)
  - Vulnerability Scan (Nessus)
  - Automatic generation of
    - Security Requirements Traceability Matrix
    - Test Plans
    - Risk assessments
    - SSAA documentation (including all appendices)
  - Workflow management
  - Executive reporting tools
- Continuous assessment of system & enterprise risk



The Xacta Solution

Software and Services That Enable Customers to Evolve From:

Information Assurance

Wireless Networking

Automated Message Handling

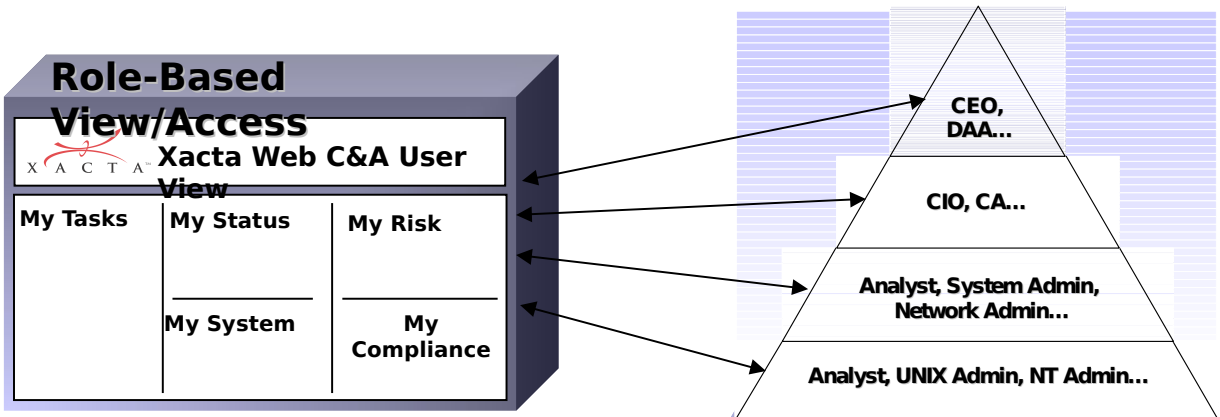
Compliance to

Enterprise Risk Management

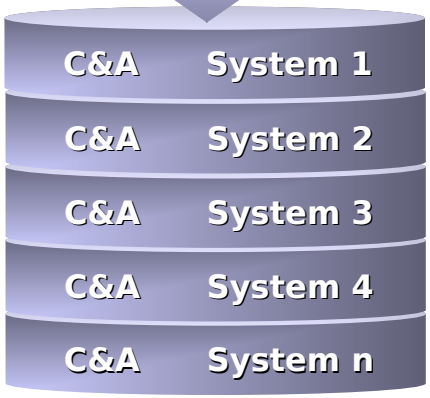
- Standards-based, C&A process compliant risk assessment
- Automated utilities for routine tasks (network discovery, inventory, system configuration, vulnerability scanning)
- Vast knowledgebase of security/agency regulations/policies correlated with test procedures
- Consistent, repeatable, efficient documentation generation capabilities

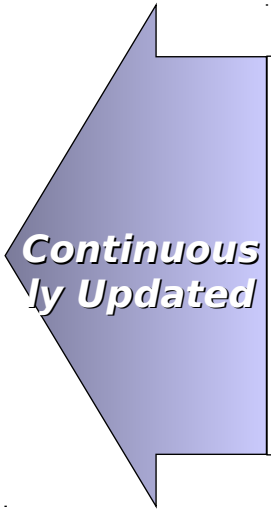
- Ability to identify change and assess its impacts on a daily or weekly basis rather than every three years
- Continuous risk profile, always-on
- Vulnerabilities matched to inventory to drive automated testing and alerts
- Hierarchical views pertinent to all levels of an enterprise; enable drill down to risk element detail and equipment configuration properties

From Compliance to Management



Management





Data Required for C&A

- Inventory
- Configuration
- Vulnerability
- Risk Levels
- Passed/Failed Requirements
- Project Schedule/Status
- Contact Info
- Other

Compliance

Information Assurance

Wireless Networking

Automated Message Handling

One Application, Many Capabilities

Information Assurance

Wireless Networking

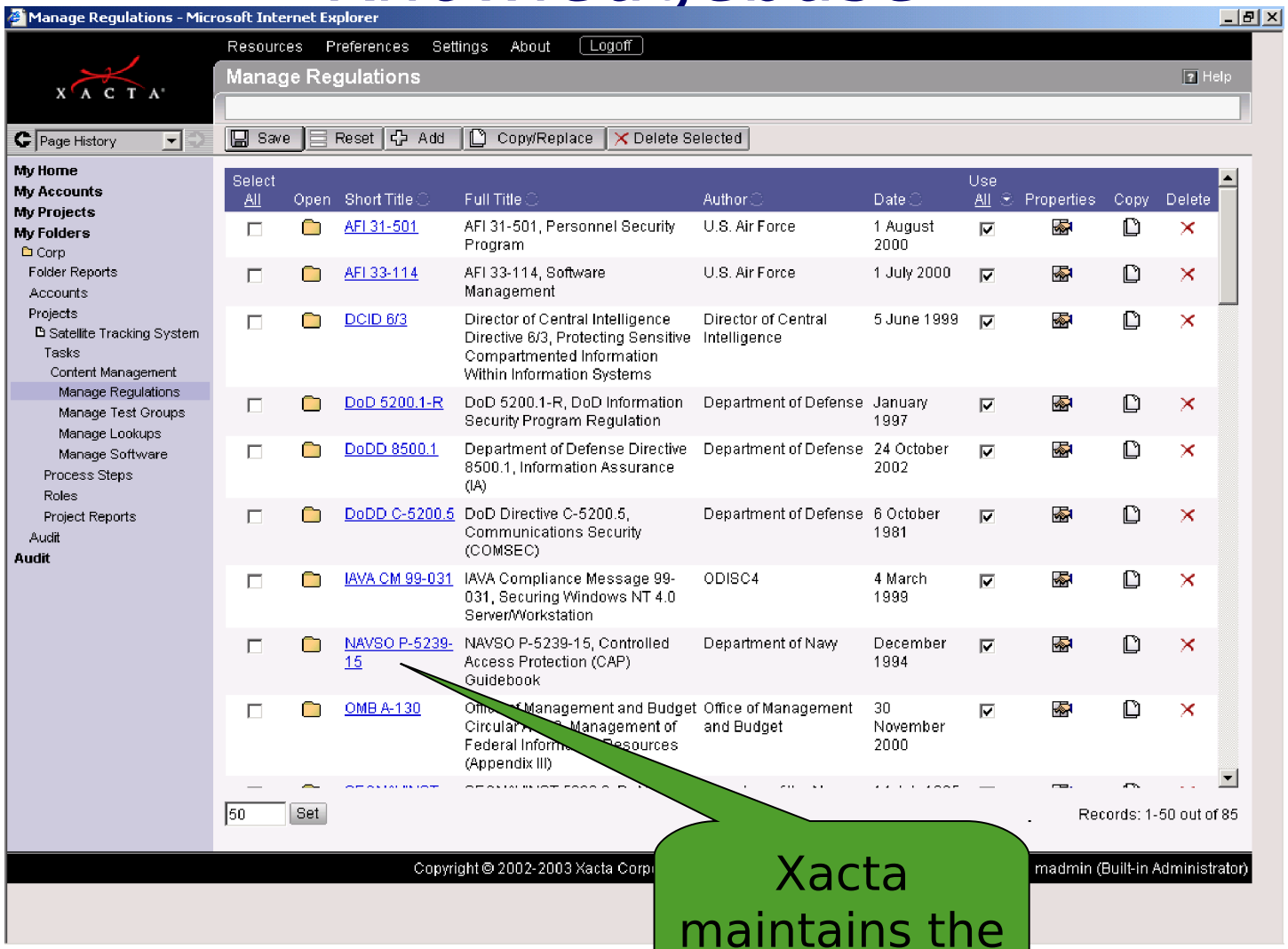
Automated Message Handling

Functional Components	Xacta Software (Component Capabilities)	OTHER PRODUCTS/VENDORS (Xacta Does/Could Work With)
Detect	• **System Discovery & OS Detection** • **Inventorying Utilities** • **Vulnerability Scanner** • **Vulnerability Notification Service**	• **DoD IAVA, DISA STIGs, Harris STAT, Securify, NESSUS, CERT Advisories, ISS, Tivoli, AF TCNO, NetRecon, SecurityAnalyst, iDefense, SecurityFocus.com, HP-OV, CA Unicenter, SecureInfo, Symantec ESM**
Protect	• **Compliance to Standards** • **Risk Calculation & Mitigation Model** • **Process Automation & Enforcement**	• **Big 5, Systems Integrators, Work Flow Product Vendors (Handysoft, Qlink, QualTrax)**
React	• **Configuration Alerts & Notifications**	• **MSSP, EM/ESM Product Vendors**
Work Flow	• **Customizable Work Flows**	• **Bizflow, Activeflow, Qlink**
Knowledgebase	• **Requirements, Regulations, Vulnerabilities, Impact Statements, Trend Data, Systems Information**	• **Boutique Security Firms, Big 5, Systems Integrators**
Reporting	• **Automated Document Publishing** • **Management & Project Status Reports**	• **Manual Templates, Crystal Reports** • **Manual Query & Reporting**
Architecture	• **Web Server (Apache/Tomcat/Catalina)** • **Database-driven** • **MS Windows & Office Compatible**	• **IBM WebSphere, MS IIS, Oracle, MS SQL, DB 2, MS Access, Solaris, Linux, HP-UX**
Consulting Support	• **Xacta Advisor Online Consulting via Chat & Email**	• **Boutique Security Firms, Big 5, Systems Integrators**

Xacta Web C&A is Tailorable to Support NMCI Legacy Transition

- Customizable workflow supports roles across multiple organizations
  - Site transition team, local DAA
  - CDA
  - EDS
  - SPAWAR (NMCI PMO, IATT, PMW-161)
  - CNNWC
- LOE/CLIN decision support
- NMCI specific IA policy
  - IA Pub 5239-13 I-III
- Custom Checklists
  - ERQ
  - NSCAP
  - Test Plans
- Custom Reporting
  - NMCI specific risk/vulnerability assessments and status reports
  - Aggregated for the site, Command, CDA, POR, FAM, DAA level
- Custom Publishing
  - CLIN specific documentation packages

DON Regulations in Knowledgebase



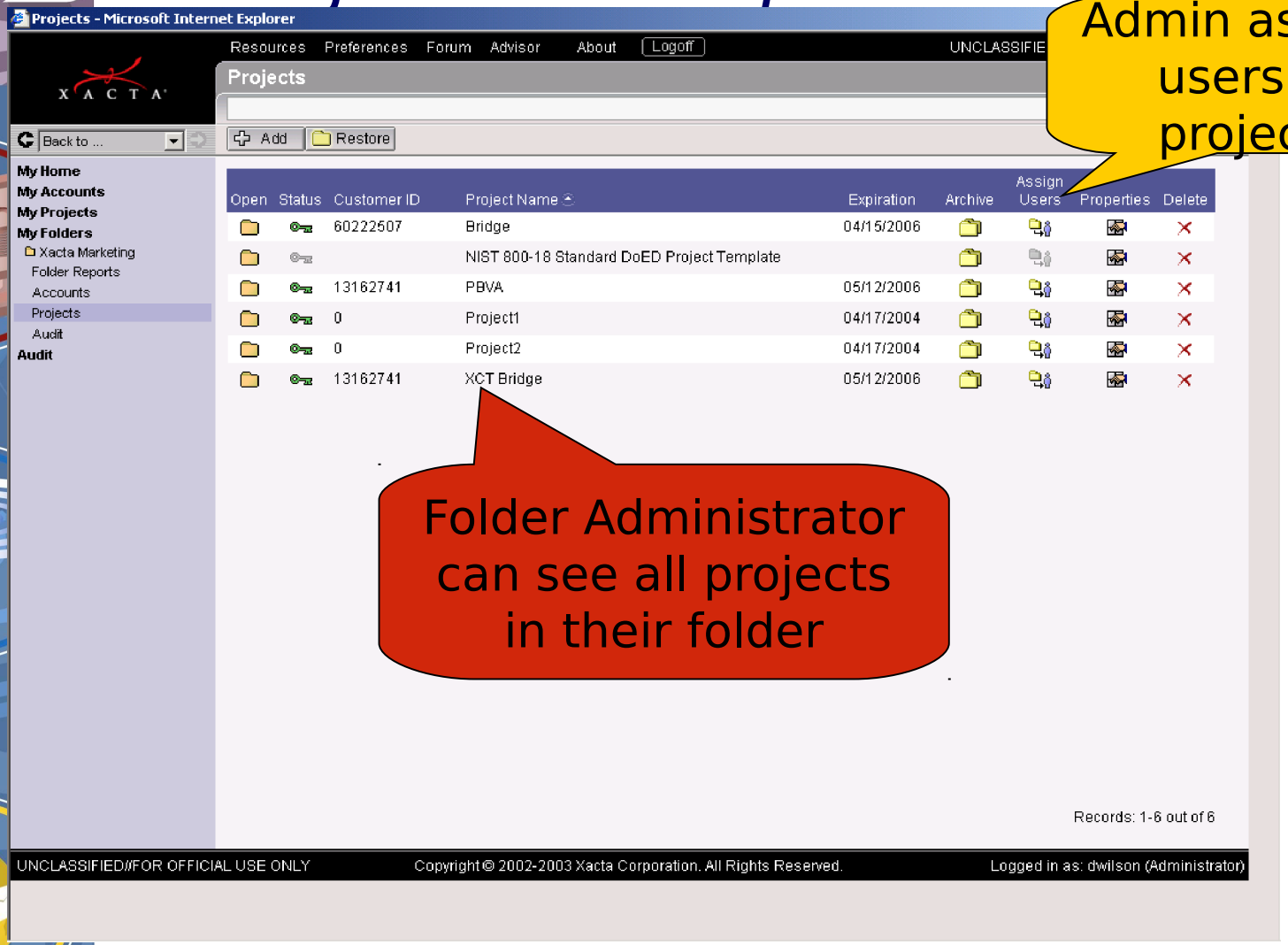
Xacta maintains the Navy content

Information Assurance

Wireless Networking

Automated Message Handling

Projects listed per User Access



Admin assigns users to projects

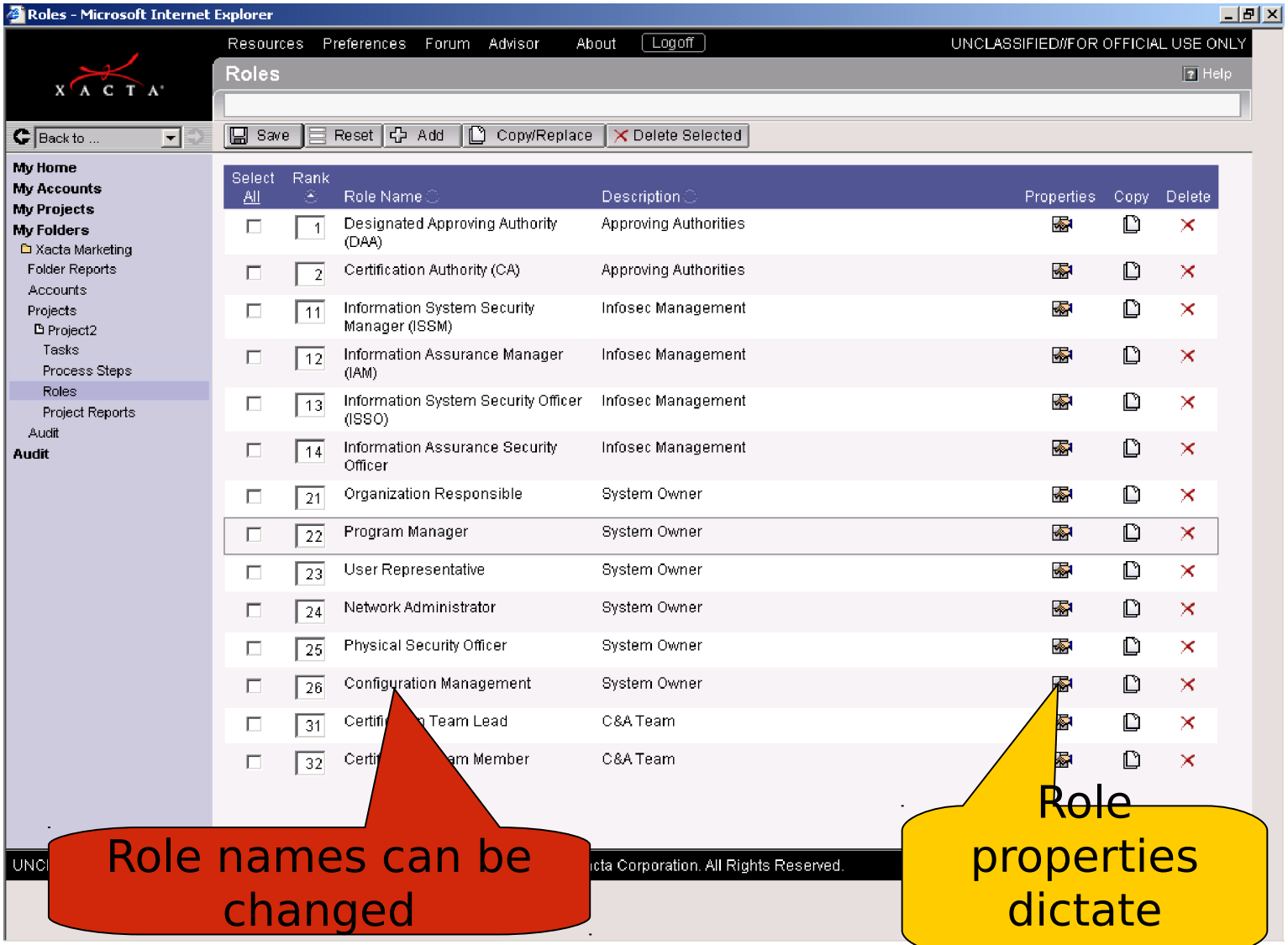
Folder Administrator can see all projects in their folder

Information Assurance

Wireless Networking

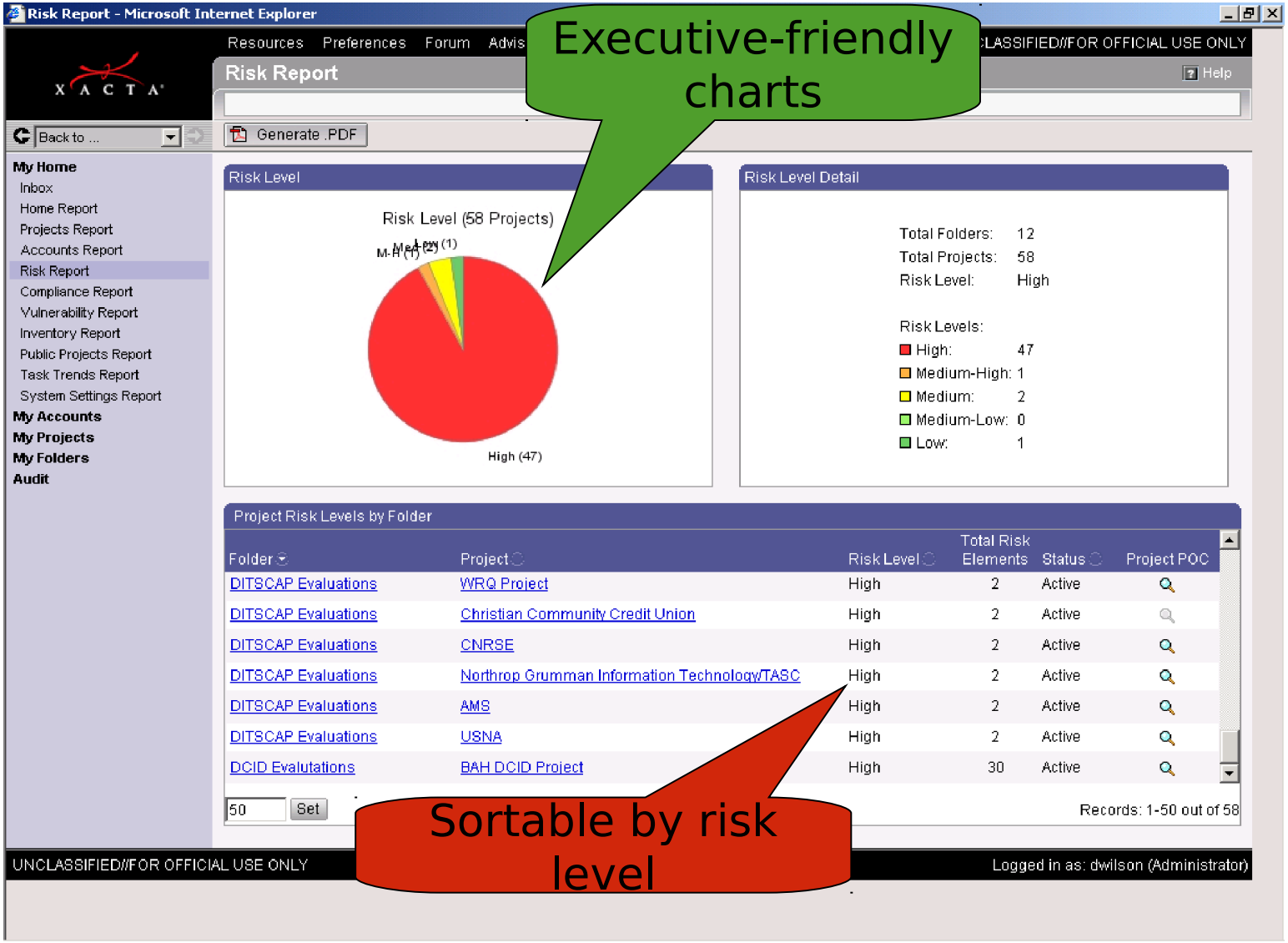
Automated Message Handling

User Access by Project Role

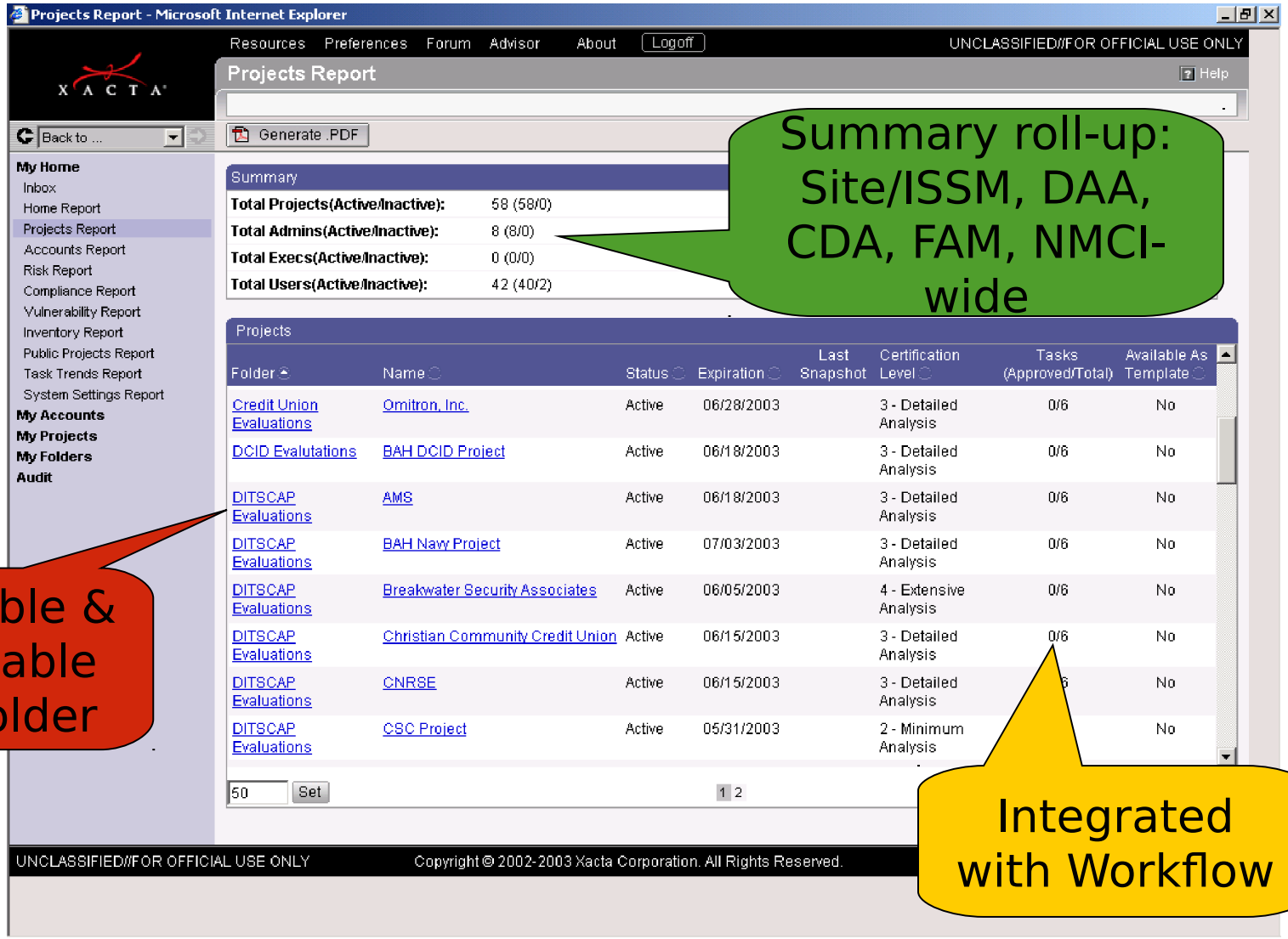


IA Situational Awareness Reporting

Information Assurance
Wireless Networking
Automated Message Handling



Portalized Project Status Reporting



Information Assurance

Wireless Networking

Automated Message Handling

More Information

- See a product demonstration of Xacta Web C&A at the Telos booth in the exhibit hall
- Consider other Telos enterprise solutions for NMCI
  - Secure Wireless Networking
  - Enterprise DMS Solution: Telos AMHS
- Contact us:

Tom Ryder
Sr. Account Manager
Telos Corporation
Tel. 703-724-4718
Fax 703-724-3865
Mobile 571-218-2223
E-mail tom.ryder@telos.com
www.xacta.com www.telos.com